Table 185 — Extended ISO 18000-7 Security IE Content

1 byte	16/8 bytes
Security Options	IV/CCM Header

- Security Options field is defined in Security Options section.
- IV/CCM Header: The initialization vector used to encrypt the frame with a symmetric algorithm.

7.3.6.1.2 Security Options

Security Options field is defined in Table 186.

Table 186 — Security Options

Bits: 0	1	2	3	4	5	6	7
Reserved	Reserved	Secure Extended ISO 0= Frame is not encrypted (there is no IV and authenti-cation field in the frame) 1= Frame is encrypted	Protection suites *See* Table 187			Reserved	PKI *See* 7.3.6.1.4 0=PKI not used 1=PKI used

The Secure Extended ISO bit, described in the above table, shall be used to indicate if the frame is secured or not. If the value of the bit 3 is:

- If the Secure Extended Mode bit is set to 1 then the frame is secured and it contains Extended Mode Security IE with Security Options and IV/CCM fields, as well as Encrypted Payload, and Authentication Data present in the frame. The Application command code and command arguments are encrypted within the Encrypted Payload field.
- If the Secure Extended Mode bit is set to 0 then the frame is NOT secured and Extended ISO 18000-7 Security IE, Encrypted Payload, and Authentication Data are NOT present in the frame. Application data containing command code and command arguments are NOT encrypted.

7.3.6.1.3 Extended Mode protection suites – Symmetric cryptography

Cryptographic protection of the Extended Mode messages consists in an optional message encryption step followed by a message authentication step. Each protection suite type is assigned an enumerated descriptor also called a protection suite identifier. A protection suite identifier is written as a designator of an encryption method followed by a designator of an authentication method:

<message-encryption-method>-<message-authentication-method>

The protection suite descriptor uniquely identifies the methods used to authenticate and encrypt the message.

Table 187 contains some of the currently considered crypto protection suites.

Table 187 — Extended Mode Protection Suites

Protection Suite Descriptor	Encryption Algorithm	Key Size, bit	Encryption Mode	Authentication Algorithm	Authentication size, # bits	Protection suites bits
AES-128-CBC-SHA1-96	AES	128	CBC	SHA1-96	96	001

Table 187 *(continued)*

Protection Suite Descriptor	Encryption Algorithm	Key Size, bit	Encryption Mode	Authentication Algorithm	Authentication size, # bits	Protection suites bits
AES-128-CBC-SHA1	AES	128	CBC	SHA1	160	010
CCM -7 (CCM for ISO/ IEC 18000-7)	AES	128	Counter	AES-CBC-MAC	64	011
HB2-128	HB2-128	128	Normal	HB2-128	16-128	100
NULL – NULL (secure bit is 0)	None	N/A	N/A	None	N/A	000

Packet Options (Protection suites bits) values 100, 101, 111 are for future extensions.

CCM-7 is based on CCM, a generic authenticated encryption block cipher mode of AES. CCM is a mode of operation defined for any block cipher with a 128-bit block size. CCM combines two well-known and proven cryptographic techniques to achieve robust security. First, CCM uses CTR for confidentiality and Cipher Block Chaining MAC (CBC-MAC) for both authentication and integrity protection.

7.3.6.1.4 Extended Mode protection suites – Asymmetric cryptography

When PKI is used, PKI bit in the Packet Options is set to 1. Protection suite bits will code the PKI algorithm used for mutual authentication:

001 ECC

010 RSA

Packet Options (Protection suites bits) values 011, 100, 101, 111 are for future extensions.

7.3.6.1.5 Encryption process

Once a device is mutually authenticated and the session keys are generated as described in 7.4.7.1 Mutual Authentication section, the device can exchange MAC data and multupurpose frames with encrypted and authenticated paylaod.

The Application layer sends a packet as defined in Table 201 with Application Header and Payload to the MAC layer. MAC layer checks the device configuration. If e.g. the device is configured to use AES for encryption and SHA1 for authentication, MAC will generate an Initialization Vector (IV) and create an Extended ISO 18000-7 Security Information Element (see 7.3.6.1.1). The Extended ISO 18000-7 Security Information element will contain the IV and Security Options - *Protection suites* field initialized with value AES-128-CBC-SHA1. The Information Element Header will be initialized with the *the Security Element Id and IE Content Length. IE List Present bit* in the Frame Control field of the MAC header will be set to one. Then, MAC will generate authentication field caculating SHA1 over the the packet received from the Application Layer, and MAC will encrypt the packet using AES algorithm with the session keys generated during Mutual Authentication Process.

Encrypted and authenticated payload of the Multipurpose/Data frame is shown in Table 188 — Encrypted and Authenticated MAC Mutlipurpose/Data Frame Payload. The size of the Authentication field depends on the selected authentication algorithms.

Table 188 — Encrypted and Authenticated MAC Mutlipurpose/Data Frame Payload

N byte	12/20/8 bytes
Encrypted MAC Payload	Authentication Data (SHA1-96|SHA1|CBC-MAC)

- **Encrypted MAC Payload:** The encrypted application layer header and payload.

- **Authentication Data:** The hash function result calculated over the payload prior to encryption.

7.3.6.1.6 Decryption process

If MAC receives a Multipurpouse/ Data frame with both ***IE List Present bit*** in the Frame Control field of the MAC header set to one and with the ***the Security Element*** present in the MAC header***.*** MAC will decrypt the payload using IV provided in ***the Security Element*** and algorithms in Security Options - ***Protection suites.*** Then MAC will re-calculate authentication field over decrypted payload and compare it with one received in the frame. If the authentication check is successful, then decrypted payload will be sent to the Application Layer. If the authentication check is not successful, the frame will be descarded.

7.3.7 Wake on Mechanisms

Following Wake on mechanisms may be supported:

- UHF Wake on
- LF Wake on
- Sensor/Alarm wake on
- Additional wake on

7.3.7.1 UHF Wake on

As defined by the ISO 18000-7, the Wake Up Signal is transmitted by the interrogator for a minimum of 2.4 seconds to wake up all tags within communication range. The Wake Up Signal consists of a 2.3 to 4.8-second 31.25 kHz square wave modulated signal called the "***Wake Up Header***" immediately followed by a 0.1-second 10 kHz square wave modulated signal called the "***Co-Header***." Upon detection and by completion of the Wake Up Signal all tags enter into the Ready state awaiting a command from the interrogator. A tag has two states, awake/ready and asleep. During the ready state, the tags accept valid commands from interrogators and respond accordingly. When the tag is asleep, it ignores all commands.

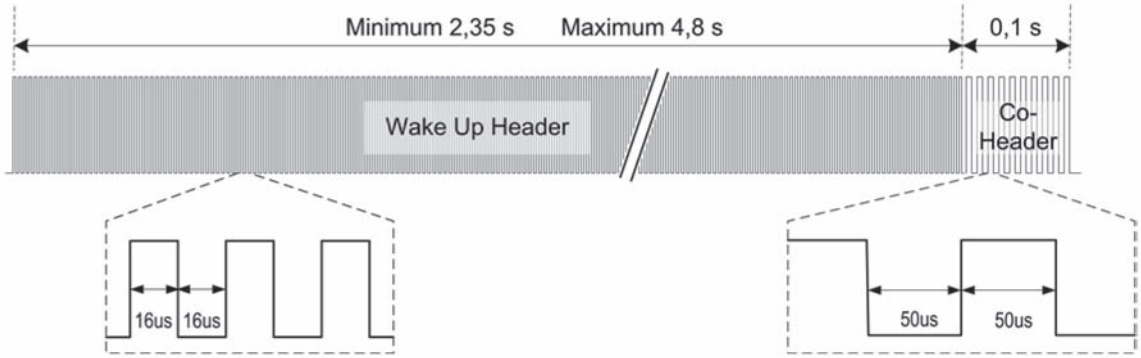

Figure 26 — Wake Up Signal

Once awoken, the tag shall stay awake for a minimum of 30 seconds after receipt of the last well-formed message packet consisting of a valid Extended protocol ID, command code, and CRC values, unless the interrogator otherwise commands the tag to sleep. If no well-formed command message is received within the 30 seconds, the tag will transition to the sleep state and SHALL no longer respond to command messages from Interrogators.

The communication between interrogator and tag shall be of the Master-Slave type, where the interrogator shall initiate communications and then listen for a response from a tag.

7.3.7.1.1 Distributed Sliding Wake-up Algorithm

Instead of sending complete 2.4 sec wakeup signal, an interrogator can distribute the wakeup signal into multiple smaller wakeup units, and distribute sending of these Distributed Wakeup Signals following the Distrubuted Wake-up Algorithm.

There two variants of the Distributed Wakeup Signal:

- One dimensional distribution of the wakeup signal
- Two dimensional distribution of the wakeup signal

7.3.7.1.2 One dimensional distribution of the wakeup signal

In ISO 18000-7, each RFID tag wakes up every 2.4 seconds and checks for a wakeup signal. If there is no wakeup signal, the tag will go back to sleep for additional 2.4 seconds. This process repeats until the tag receives the wakeup signal and wakes up. In the context of this algorthm, 2.4 second interval is called „wakeup super frame“

The 2.4 second interval, can be sub-divided into multiple beacon intervals, e.g. 24 intervals with 100 millisecond duration each. In a beacon enabled RF network, the interrogator shall send a beacon frame periodically every beacon interval. The interrogator will distrubute wakeup signal and embed the wake-up procedure into normal operating cycle.

One of the 100 millisecond beacon intervals from total of 24 in each wakeup super frame, will be dedicated to 100 millisecond wakeup signal. The wake-up signal is distributed between multiple wakeup super frames. In the first (index 0) wakeup super frame, the wake up signal will occupy beacon interval 0. In the second (index 1) wakeup super frame, the wake up signal will occupy the beacon interval 1. In the third (index 2) wakeup super frame, the wake up signal will take the beacon interval 2. Since the wake-up, a 100 millisecond interval slides, in the last (index 23) wakeup super frame, the wake up signal will occupy beacon interval 23. After each of the 100 millisecond wake-up signals, the RFID interrogator can perform the collection procedure of the woken up tag group before sending the next wake up signal.

It takes 24 wake-up intervals (100msec each) to wake up all tags.

In 57.6 sec all tags will be woken up and possibly collected. This would guarantee that newly arrived tags will be woken up (discovered) in 57.6 seconds (24 X 2.4sec = 57.6 sec).

Overhead for sending distributed-sliding wake-up signals is 1/24 equals 4.17%.

Figure 27 depicts the Distributed Sliding Wake-up algorithm for 100 millisecond beacon interval.

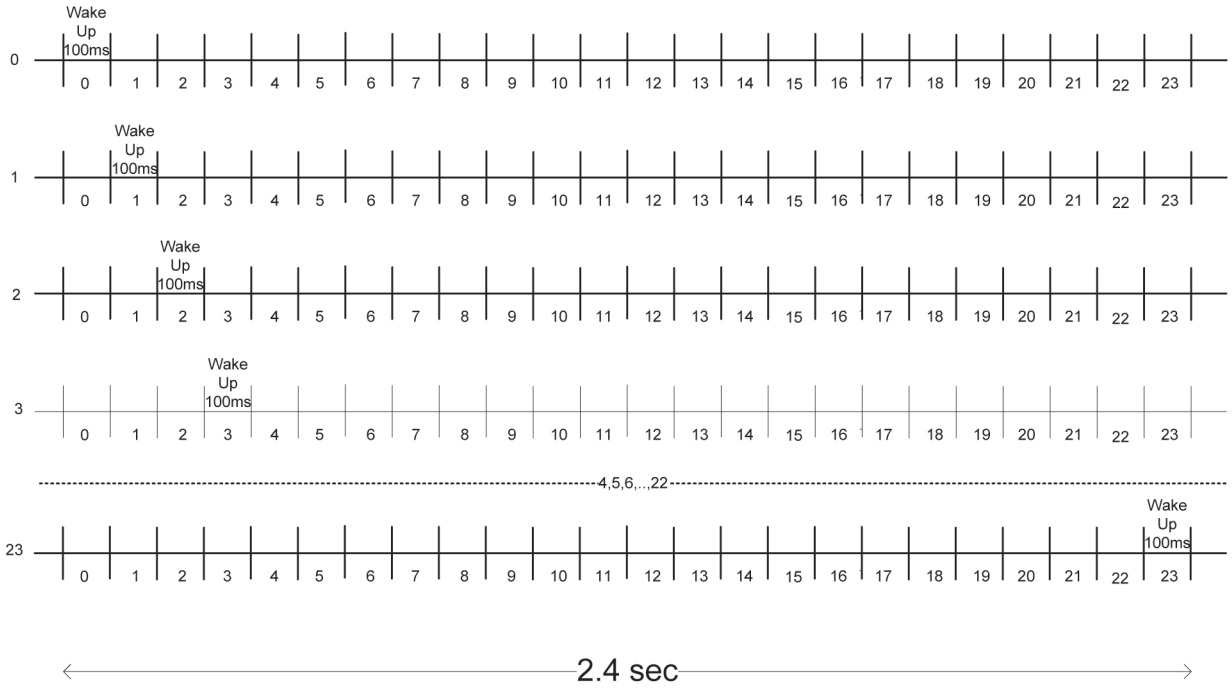

Figure 27 — Distributed Sliding Wake-up Algorithm

We assume that the wakeup interval slides in the frames 4 to 22 from slot 4 to slot 22.

The interrogator can take multiple of 2.4 second intervals for collection of a group of woken up tags between two sliding wake-ups. It is important that next 100msec wake up interval slides, so the next group of tags can be woken up.

Note: if the network is configured to be in beconless mode of operation, the intorrogator will not be sending beacons, and the distribution of the wakeup signal will remain the same as described.

7.3.7.1.3 Two dimensional distribution of the wakeup signal

In beacon enabled networks the wakeup signal can be reduced bellow a beacon interval. In Figure 28 the wake up signal is 1/6 of the beacon interval. In each wakeup super frame, the wakeup signals slide inside each beacon interval. The wakeup signal is distributed in two dimensions, both in a beacon interval and in a wakeup super frame, Figure 28 The RFID devices are divided into 24 groups, although the super frame is divided into 4 beacon intervals. In one dimensional distribution of the wakeup signal, there would be only four groups of devices. Two dimensional distribution shall even further better address the issue of evenly waking up a population of a large number of tags.

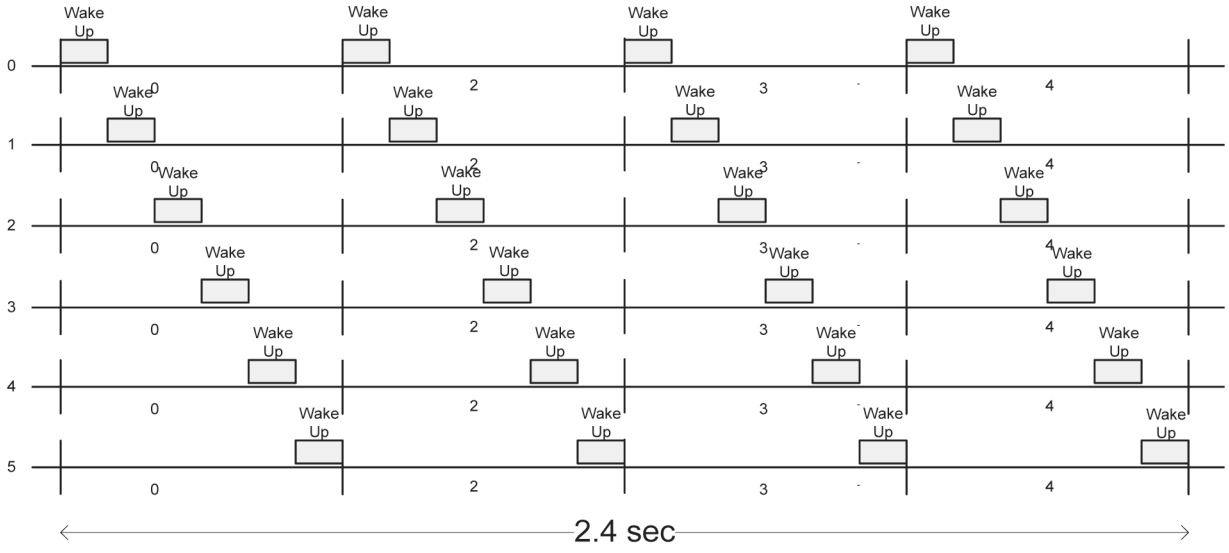

Figure 28 — Two dimensional distribution of the wakeup signal

Note: if the network is configured to be in the beconless mode of operation, the intorrogator will not be sending beacons, and the distribution of the wakeup signal will remain the same as described.

7.3.7.1.4 Distributed Wake-up Signal in Extended ISO 18000-7

Existing ISO 18000-7 defined Wakeup signal with scaled down Wake-Up Header and Co-Header duration can be used re-used for Distributed Sliding Wakeup Algorithm as presented in the Table 189 — Distributed Wakeup Signals.

Table 189 — Distributed Wakeup Signals

Wake Up Type	Wake Up Header square wave modulated signal		Co-Header square wave modulated signal	
	Duration	Frequency	Duration	Frequency
ISO 18000-7 Wakeup signal	2.3 to 4.8-second	31.25 kHz	0.1-second	10 kHz
Distributed Wake Up signal	T_{FW} = Configurable <=1.2 sec	F_{FW} 31.25 kHz	T_{FC} <= 0.1 second	F_{FC} = 10 kHz

7.3.7.2 LF Wake-On

The Low Frequency (LF) link supports short range communication from an exciter to the tag. This LF link enables the system to wake-up the tag and issues commands to the tag. As LF is a one-way link, the tag's response to the LF command is transmitted through the UHF link making use of the Extended Mode PHY, MAC and Application framework.

7.3.7.2.1 Exciter to Tag Communication (LF link)

The exciter to tag communication utilizes low frequency (122.64 kHz) AM modulation scheme and operates at short range. Data is transmitted from the exciter to the tag without acknowledgment over LF (one way LF communication link).

7.3.7.2.1.1 Data modulation and coding

Data transmitted between the exciter and the tag utilizes OOK scheme with two distinctive signal levels (RF carrier frequency being switched on or off).

7.3.8 Preamble

The preamble shall be comprised of eight (8) cycles each 16T period long (where T = 1/32768 sec). The preamble shall start with signal high and then alternating between 8T high and 8T low periods.

The preamble shall be preceded by RF Burst (RF ON) of minimum duration of 48T followed by 8T of signal low (RF OFF). Refer to Figure 2

Note that when multiple packets are being transmitted back to back the RF Burst signal is required to be transmitted only for the first transmitted packet.

7.3.9 Data bytes

Data bytes shall be in Manchester code format, each byte is comprised of 8 data bits. The data bit period shall be 16T (where T = 1/32768 sec), the total byte period shall be 128T. A falling edge in the centre of the bit-time indicates a 0 bit, a rising edge indicates a 1 bit.

7.3.10 Packet end period

A final period of 24T of continuous high, followed by a 24T continuous low and followed by minimum of 8T high shall be transmitted after the last Manchester encoded bit within the packet.

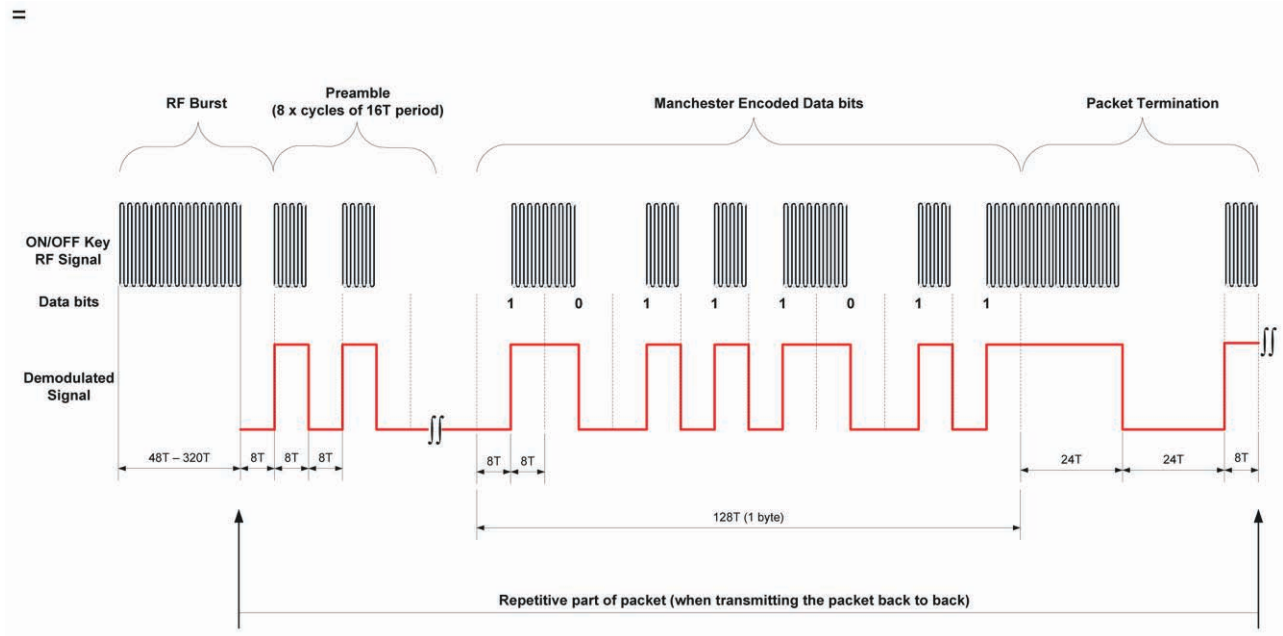

Figure 29 — Data Modulation

The bit period shall have duration of 16T, where T = 1/32768 seconds with an error tolerance of +/-3%. This symbol rate of produces effective data rate of 2.048 kb/s.

The packet structure is as shown in Figure 31.

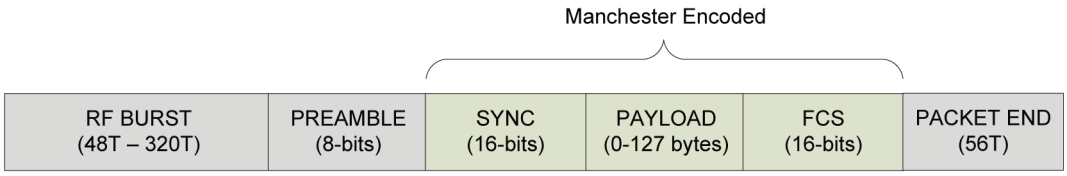

Figure 30 — Packet Structure

Notes:

The order of transmitted Data bytes is in accordance with 802.15.4e MAC specification.

The packet transmission starts with transmission of carrier signal (CW) in duration of 48T periods to 320T periods. Acctual duration of CW transmission is application dependant and can be used to trade off RFID tag response time versus its power consumption.

Peramble field (P) follows CW signal and is 8 bits long (all “0” when Manchester encoded).

Sync Word field serves to detect start of frame and shall be 0x115F (binary value = 0001 0001 0101 1111) . The Preamble of 0x00 and Sync Word of 0x115F work together to provide accurate start of packet (start of frame delimitation).

A CRC checksum shall be calculated as a 16-bit value for each packet, initialized with all zeroes (0x0000), over entire payload bytes (excluding preamble and sync word) according to the CCITT polynomial (x16 + x12 + x5 +1). The CRC shall be appended to the data included in the command message as a two bytes field. Reference: ITU-T Recommendation V.41 (Extract from the Blue Book), Code-independent error-control system, Appendix I - Encoding and decoding realization for cyclic code system.

7.3.10.1.1.1 Protocol

The type and amount of data being transmitted from the exciter to the tag is dependent on the particular application. Several modes of operation are being defined to provide flexible message structure to meet various application requirements.

7.3.10.1.1.2 Message structure

The exciter to tag communication protocol uses byte oriented, packet based message structure utilizing 16-bit Frame Check Sequence (FCS) error detection mechanism for reliable communication. The protocol utilizes 16-bit mode field prefix that defines the message structure and optimizes the packet size that is being sent to the tag.

The message structure with all the fields is shown in Table 190.

Table 190 — Payload message structure

LF Mode	Application ID (Optional)	Tag ID (Optional)	Exciter ID	LF RSSI (Optional)	Exciter Time-out (Optional)	Command Code (Optional)	Parameters (Optional)	
8-bits/16-bits	8-bits	48-bits / or 64-bit IEEE ID	16-bits	8-bits	8-bits	8-bits	Variable	16-bits

Notes:

The transmission of the packet fields within the message starts with the LF Mode field and ends with the FCS field. The most significant bit within each byte is sent first. Lower order byte is sent first within each field. The FCS calculation includes all bytes in the packet except itself.

7.3.10.1.1.3 LF Mode field

The LF mode field bits are defined Table 191

Table 191 — LF Mode field (byte 1)

Value	'0'	'1'	Definition
bit 0	No Application ID	Application ID	This bit indicates whether the Application ID is included or excluded from the message.
bit 1	No Tag ID	Tag ID	This bit indicates whether the Tag ID field is included or excluded from the message.
bit 2	48-bit Tag ID	64-bit IEEE ID	This bit indicates whether 48-bit Tag ID or 64-bit IEEE address is being used..
bit 3	LF RSSI threshold not used	LF RSSI threshold used	This bit indicates whether LF RSSI threshold value (1 byte) is included in the message. The RSSI threshold level informs a tag on boundary of the LF field at which it shall respond (tag's measured LF RSSI is greater than LF RSSI threshold). If the measured RSSI is lower than provided LF RSSI threshold a tag will not respond. If this field is not included in the message a tag shall respond to all correctly received LF messages regardless of the signal level.
bit 4	No Command	Command	This bit indicates whether the Command and associated parameters fields are included in the message.
bit5 & bit 6	LF Sequence ID		LF Sequence ID is used to identify all identical messages sent by the exciter as a part of the same transaction (same Sequence ID).
bit 7	Extension Mode byte not included	Extension Mode byte included	This extension bit is used to expand LF Mode byte with additional 8-bit of bitmapped link control bits. If 2nd LF Mode byte is not included than it is assumed that bit options defined in 2nd LF Mode byte are set to zero.

The LF mode field bits are defined Table 191

Table 192 — LF Mode field (byte 2)

Value	'0'	'1'	Definition
bit 0	Exciter Timeout not used	Exciter Timeout is used	Exciter Timeout field is included in the packet.
bit 1	Exciter IN	Exciter IN and OUT	This option instructs the tag to generate one or two types of UHF responses depending on the operational scenarios. If Exciter IN and OUT response is selected than tag will send two UHF messages, IN when entering the Exciter field and OUT when leaving the Exciter field. If Exciter IN response is selected than the tag will generate only IN UHF message as it passes through the Exciter.
bit 2	Reserved	Reserved	
bit 3	Reserved	Reserved	
bit 4	Reserved	Reserved	
bit 5	Reserved	Reserved	

Table 192 *(continued)*

Value	'0'	'1'	Definition
bit 6	Reserved	Reserved	
bit 7	Reserved	Reserved	

7.3.10.1.1.4 Message Parameters

- Application ID indicates the tag command set to be used. If this field is not included in the message, the Application ID is defaulted to 0x02.
- Tag ID is the 48 bit or 64-bit ID of the target tag, depending if Base Mode addressing or IEEE EUI-64 addressing is used
- .
- Exciter ID is a 16-bit number that uniquely identifies the exciter. The range of the Exciter IDs is from 1 to 2^{16}-1. The Exciter ID zero is reserved.
- Exciter Timeout represents the exciter OFF time during its periodic transmission. It is used to prevent the tag to retransmit the same message for every exciter transmission cycle. The range of the Exciter Timeout is from 1 to 255 seconds.
- Command Code follows a simple structure with only two main command categories:
- Write to the tag
- Read from the tag

Where command format is defined as follows:

Table 193 — Command format

Command prefix (1-bit)	Tag Command code (7-bits)
1 – Write 0 – Read	*See Section 7.3.10.1.1.5.*

Parameters is a variable length field that contains the parameter(s) associated with the LF Command. The length of the parameter field is derived based on the command code and is not explicitly specified.

7.3.10.1.1.5 Tag Command Code

The exciter can issue tag commands from multiple tag command sets. The Application ID indicates the tag command set to be used.

Table 194 describes the default tag command set that is associated with Application ID 0x02. Note that if no Application ID is included in the LF packet, this default tag command set should be assumed. The definition of additional tag command sets is outside of the scope of this specification.

Default tag command set:

Table 194 — Default tag command set for Application ID 0x02

Tag Command Codes	Tag Parameter Name	Tag Parameter Size [bits]	Parameter Type Description	R/W Status
0x07	User ID byte length	8	User ID byte length indicates the length of the ISO User ID data field. When the User ID Length is set to 0 the User ID is disabled and will not be reported within the UHF response message.	R
0x0B	Tag type	8	Tag Type is used to distinguish various tag models and is manufacturer specific.	R
0x0E	Wake Up	-	This command is only applicable for tag that supports 2-way UHF communication. Upon reception of this command tag will turn on UHF receiver and listen for incoming UHF command from the Coordinator.	-
0x31 / 0xB1	Tag transmission period under the Exciter field	1+15	The most significant bit is used to enable or disable tag periodic exciter IN transmissions while tag is still under Exciter LF filed. The lowest 15 bits indicate period in seconds. If all 15 bits are zero than no change in transmission rate is assumed and only most significant bit is used to enable or disable transmission rate.	R/W
0x32 / 0xB2	Tag beacon transmission period	1+15	The most significant bit is used to enable or disable periodic tag beacon transmission. The lowest 15 bits indicate period in seconds. If all 15 bits are zero than no change in transmission period is assumed and only most significant bit is used to enable or disable transmission rate.	R/W
0x43 / 0xC3	Manufacturer specific.			
0x98	Manufacturer specific.			
0x99	Manufacturer specific.			
0x9A	Manufacturer specific.			
0x2A / 0xAA	Manufacturer specific.			

7.3.10.1.2 Tag Response (UHF link)

The tag's response to the LF packet is encapsulated within an Application Data Packet and is carried by the MAC layer using MAC Data frame or MAC Multipurpose frame.

The data being sent to the coordinator has a different format depending on the mode of operation. The LF response application payload format is shown in Table 195.

Table 195 — LF response appliation payload format

Application ID	Tag Status	Tag ID	Exciter ID	LF RSSI (Optional)	User ID (Optional)	Command Code (Optional)	Command Arguments (Optional)
8-bits	16-bits	48-bits / 64-bit IEEE ID	16-bits	8-bits	16-bits	8-bits	Variable